1. **What should Alice transmit to Bob assuming we are restricted to public key cryptosystems? Use the notation above.**

Alice will transmit EK(Pu(B),M1).

1. **When large messages must be encrypted, symmetric key cryptography is usually preferred to public key cryptography. Explain why.**

symmetric key cryptography is usually preferred because it is faster and requires less computational power (makes it more suitable for large data encryption).

1. **What should Alice transmit to Bob, to enable Bob to verify that it was indeed Alice who sent the message. Use the notation above. Do not worry about computational efficiency concerns.**

For Bob to know the message is from allice, she can digitally sign it with her private key Pr(A). transmitting M1,EK(Pr(A),M1)

1. **If computational efficiency is a concern, what should Alice transmit to Bob to enable him to verify it was Alice who sent the message? Use public key cryptography along with other mechanisms as appropriate**

Public key cryptography is slow, to help she could sign only with a hash of her message, instead of the full message.

She can compute hash of M1 by H(M1)

She signs the hash using her private key, bob knows it is her:

EK(Pr(A),H(M1))EK(Pr(A), H(M1))EK(Pr(A),H(M1))

Bob then verifies by computing the hash of M1

H(M1)

Then decripts alices signature by:

DK(Pu(A),EK(Pr(A),H(M1)))=H(M1)

If this matches the decrypted hash, its alices. Doing this is mor efficient as signing just the hash is more efficient than signing the whole message